

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
GREENEVILLE DIVISION

FILED

MAY 08 2019

Clerk, U. S. District Court
Eastern District of Tennessee
At Greeneville

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
KSP00N73@ICLOUD.COM THAT IS
STORED AT PREMISES CONTROLLED
BY APPLE, INC.

2:19-MJ-

143

JUDGE CORKER

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

Your Affiant, Cameron L. Miller, Special Agent, United States Bureau of Alcohol,
Tobacco, Firearms and Explosives (ATF), being first duly sworn under oath, states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant makes this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple, Inc., (hereafter, "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. Your Affiant, a Special Agent with ATF, an agency of the United States Department of Justice, has been so assigned since January of 2015, and, therefore, is an officer of the United States who is empowered to conduct investigations of, and to make arrests for, the offenses enumerated in United States Code, Titles 18 and 26, and to request warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

3. Your Affiant has specialized training and/or experience in the area of illegal firearms possession, firearms trafficking, drug distribution, gangs, undercover operations, surveillance and debriefing informants and suspects. All references herein to any experience refers to experience gained through training, conducting firearms and controlled substances investigations, and participating in those investigations with other experienced investigators, as well as conversations with other law enforcement officers.

4. Prior to 2015, your Affiant was employed as a sworn law enforcement officer in North Carolina for approximately seven years, including work experience as a Drug Enforcement Administration (DEA) Task Force Officer, Vice/Narcotics/Gang Detective, and Patrol Police Officer. As an ATF Special Agent, your Affiant was assigned and worked complex criminal investigations in the Puerto Rican Field Office, the St. Thomas, USVI Satellite Office, and the Memphis, TN Field Office, and is presently assigned to the Satellite Office of ATF's Nashville Field Division in Greeneville, TN.

5. Your Affiant has participated in, and has been assigned to, multiple investigations involving illegal firearms possession and manufacturing, illegal destructive device possession and manufacturing, and federal crimes of violence. Presently, your Affiant's primary assignment is to conduct investigations involving firearm offenses, firearms trafficking, violent crimes, drug trafficking, and money laundering occurring throughout the Eastern District of Tennessee. This includes, among other things, conducting investigations of organizations trafficking firearms, individuals illegally possessing or making firearms, violent gangs, firearm offenses, and narcotics violations.

6. Through training, investigations and experience, your Affiant has taken part in cases relating to the trafficking of firearms, the use and possession of firearms by persons prohibited by law, and the possession of illegal firearms and firearms parts, and is familiar with and has participated in various methods of investigations, including, but not limited to: electronic surveillance, physical surveillance, interviewing and general questioning of witnesses, use of confidential informants and use of cooperating witnesses. Your Affiant has debriefed confidential informants and cooperating witnesses regarding the habits and practices of people engaged in the illegal trafficking of firearms. Furthermore, your Affiant has conducted and participated in numerous investigations to include: crime scene investigations, collection of evidence, interviews and the execution of search warrants.

7. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of 18 U.S.C. § 922(g)(1), as described in Attachment B.

PROBABLE CAUSE

8. On April 16, 2019, deputies of the Hawkins County Sheriff's Office (HCSO) responded to 218 Massengill Avenue in Bulls Gap, Tennessee to investigate a disturbance. The HCSO dispatch received a call from Wendy Sexton, a resident of that address, stating that a male was at her residence causing a disturbance. Corporal Stacy Vaughn of HCSO arrived on the scene and began speaking to Sexton and her boyfriend, Kenneth Todd Spoon (SPOON). Corporal Vaughn learned that a male friend of SPOON's, who was creating the disturbance, had left prior to the arrival of deputies. The male reportedly left the residence through the rear of the property after learning that he had outstanding arrest warrants and law enforcement was on the

way to the house. Corporal Vaughn, assisted by Sergeant Jeremy Nash of HCSO began looking in the area for the wanted male.

9. Corporal Vaughn returned to the Sexton residence to find Sexton and SPOON in a verbal argument. While dealing with SPOON and Sexton, SPOON began telling Sexton to remove firearms from the house since he was a convicted felon. Deputies learned that SPOON has prior convictions, including, the felony offenses of: "Aggravated Assault" in Hamblen County, TN in 2012; "Attempted Aggravated Robbery" in Cocke County, TN in 1997; "Escape" in Hamblen County TN in 1995; and "Burglary" in Hamblen County, TN in 1994.

10. SPOON stated to Sexton that she should get her firearms out of the house. Sexton inquired, "My firearms?" She then asked SPOON, "So they're my firearms?" SPOON confirmed that the firearms being referenced were hers. Sexton asked law enforcement if she could get the firearms and she was given permission. Sexton brought a black case up to the carport area from a downstairs bedroom of the residence. She opened up the rifle case and showed deputies the contents. The case had high capacity magazines, ammunition, and the following, four firearms:

- a. Taurus PT-22, .22 caliber pistol,
- b. SKS, 7.62x39 caliber rifle,
- c. Masterpiece Arms, 9mm pistol, and
- d. Smith & Wesson, M&P 15, .223 caliber rifle.

11. Due to the type of call, volatility of the situation, the presence of several firearms, loaded, high capacity magazines, and ammunition, the apparent absence of a wanted male who left prior to the arrival of deputies and who was not located in the area around the residence, and SPOON's statements regarding firearms in the residence, deputies believed a protective sweep of

the residence was necessary. In addition, law enforcement sought consent from Sexton and SPOON for entry into the residence. When asked for consent, SPOON stated, "I'd rather you not, but it's her house." Sexton signed a consent form and deputies entered the residence to conduct a protective sweep of the residence for their safety as well as that of the civilians present.

12. During the protective sweep, deputies observed, in plain view, ammunition in the master bedroom, as well as a Ruger, .380 caliber, pistol, on the floor, beneath a raised bedframe¹. Several rounds of ammunition were on the nightstand to the right side of the bed, which is the side of the bed where SPOON reportedly sleeps. The ammunition was laying on top of men's shorts with other personal items. Deputies found one (1) round of ammunition beneath the raised bedframe. SPOON's girlfriend told law enforcement that the Ruger, .380 pistol belonged to her.

13. The firearms and ammunition brought out of the house by Sexton were not secured in a locked case or otherwise secured from SPOON's access. Tennessee Code Annotated § 39-17-1307 prohibits possession of a firearm by a person convicted of a felony involving the use or attempted use of force, violence, or a deadly weapon, or a felony drug offense. Deputies believed there was sufficient probable cause to believe that SPOON was in possession of a firearm in violation of T.C.A. § 39-17-1307, so they arrested him and transported him to the Hawkins County Sheriff's Office for an interview.

14. At the time of his arrest, SPOON was in possession of an Apple, iPhone X, which was secured in HCSO evidence.

¹ Law enforcement later learned that, during the argument with the male who was refusing to leave the residence, Sexton had exited the house and discharged the Ruger, .380, pistol.

15. On the same date of the arrest, your Affiant conducted a custodial interview of SPOON at HCSO jail. After being advised of his rights under *Miranda* and subsequently waiving those rights, SPOON provided the following information:

He has lived with Sexton at the residence for over a year and sleeps in the master bedroom. He admitted to possessing the firearms found downstairs in the residence. He described his possession of the firearms as strictly to instruct Sexton's adult son on how to clean the firearms. He was familiar with the types of firearms found, including their caliber, parts, accessories and function (semi-automatic versus fully automatic). In response to the ammunition found upstairs in his bedroom, he stated, "Yeah from time to time, there might be some laying around." He admitted to taking the adult son of Sexton to a private property of a third party to shoot firearms. He stated that his girlfriend found the ammunition laying around the house and placed it on his dresser.

16. Additionally, since his arrest by HCSO, SPOON has been video and audio recorded on jail calls and visitation video speaking to Sexton. SPOON admits in recorded calls that he possessed the firearms to teach Sexton's son firearm safety.

17. Based upon SPOON's admissions of possessing firearm and ammunition, the evidence collected by HCSO, and his status as a convicted felon, your Affiant charged SPOON via Federal complaint with being a felon in possession of a firearm and ammunition. This Court arraigned him on the Complaint on April 24, 2019, and his custody transferred to the U.S. Marshals Service. He has remained in custody since his arrest on April 16, 2019.

18. Your Affiant learned through a confidential source (CS) that SPOON was in possession of a firearm and ammunition sometime after March 8, 2019. This possession took place on private property in the Eastern District of Tennessee. While there, SPOON was video-recorded shooting a firearm and, therefore, possessing ammunition. The CS informed your Affiant that the

video recording of SPOON shooting the firearm was sent to at least one person via text messaging service on the Apple, iPhone X that SPOON uses. Your Affiant has viewed the video and it depicts SPOON shooting a firearm. Your Affiant secured the Apple, iPhone X from HCSO and it is now in the vault at ATF's office in Greeneville, TN.

INFORMATION REGARDING APPLE ID AND iCloud²

19. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

20. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

² The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at <https://support.apple.com/kb/PH26502>.

c. iCloud is a file hosting, storage, and sharing service provided by Apple.

iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and

synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. Apple's App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

21. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

22. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

23. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated

with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

24. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

25. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition,

information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

26. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

27. Your Affiant has viewed the video of SPOON possessing and shooting a firearm, which, your Affiant was informed by a CS, was sent from SPOON's Apple iPhone X. Your

Affiant believes that, based on training and experience, digital evidence such as video, photographs, emails, and text messages of SPOON's possession of a firearm, ammunition, and an unregistered machine guns may be stored on the iCloud. Additionally, meta data related to the location of where the images or videos were taken may be stored. In your Affiant's training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

28. The original video and photograph files may be stored in the iCloud. This may be relevant to identify the specific location, date, and time of the illegal activity. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on your Affiant's training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

29. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and

because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

30. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

31. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

32. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. Your Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

34. Based on the forgoing, your Affiant requests that the Court issue the proposed search warrant.

35. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such court) . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

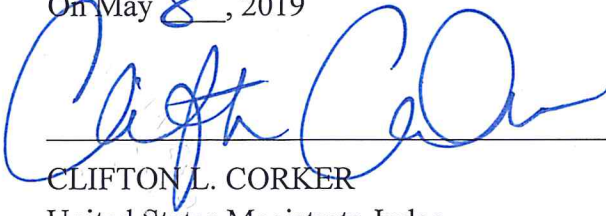
36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Cameron L. Miller, Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Subscribed and Sworn to before me
On May 8, 2019



CLIFTON L. CORKER
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with kspoon73@icloud.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple, Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within no more than 14 calendar days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 922(g)(1) involving Kenneth Todd Spoon since March 8, 2019 to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.